UNITED STATES MARINE CORPS
25TH MARINE REGIMENT
4TH MARINE DIVISION, FMF
MARINE FORCES RESERVE
4 LEXINGTON STREET, BOX 140
FORT DEVENS, MASSACHUSETTS 01434-4476

1000
S-6
19 JAN 07

REGIMENTAL POLICY LETTER 7-07

From: Commanding Officer
To: Distribution List

Subj: OFFICIAL USE OF GOVERNMENT INFORMATION TECHNOLOGY RESOURCES

Ref: (a) MARADMIN 162/00
(b) DD Form 28575
(c) DISA Information Assurance Website: http://iase.disa.mil/index2.html

Encl: (1) Information Assurance Check List for Government Network Devices

1. PURPOSE. To promulgate guidance for usage of computers, the Internet, and all other related information technology with 25th Marine Regiment.

2. OFFICIAL USE. Government information technology resources are for official use and authorized purposes only. Use of these resources, to include access to the Internet, is authorized when work related and determined to be in the best interests of the federal government and the Marine Corps. Use should be appropriate and related to assigned tasks. Examples include, but are not limited to, using these resources to:

a. Obtain information to support Department of Defense, Department of the Navy, and United States Marine Corps missions.

b. Obtain information that enhances the professional skills of Marine Corps personnel.

c. Improve professional or personal academic education or military/civilian professional development program.

d. For incidental personal purposes such as Internet searches and brief communications, as long as use:

(1) Does not result in added costs to the government.

(2) Does not adversely affect the performance of official duties by the user.

(3) Serves a legitimate public interest such as enhancing professional skills or improving morale.

(4) Is of minimal frequency and duration and occurs during an individual's personal time.

e. Does not overburden government computing resources or communication systems.

f. Is not used for purposes that adversely reflect upon the Marine Corps.

3. PROHIBITED USE. Examples of prohibited use include, but are not limited to, the following:

a. Illegal, fraudulent, or malicious activities.

b. Partisan political activity, political or religious lobbying or advocacy of activities on behalf of organizations having no affiliation with the Marine Corps or Department of Defense.

c. Activities whose purposes are for personal or commercial financial gain. These activities include solicitation of business services or sale of personal property.

d. Unauthorized fundraising.

e. Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography or hate literature.

f. Obtaining, installing or using software obtained in violation of the appropriate vendors patent, copyright, trade secret, or license agreement.

g. Creating, forwarding, or passing of chain letters.

h. Downloading of music, movies, or pictures for personal purposes.

i. Gambling, playing online games, or participating in online social gatherings.

h. Installing shareware, spyware, or software that detects usage and reports to external company or organization.

i. Illegal, fraudulent, or malicious activities.

4. Applicability.

a. This instruction applies to all personnel, military and civilian, within 25th Marine Regiment. Personnel are individually responsible for compliance. This instruction establishes the standard that is to be followed by all personnel, military or civilian within 25th Marine Regiment. Military personnel are subject to disciplinary action under the Uniform Code of Military Justice if they knowingly, willfully or negligently violate the provisions of this instruction.

b. Civilian employees, are subject to criminal penalties under applicable Federal statutes, as well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of this instruction.

5. Required Action. Unit Information Systems Coordinator representatives will establish an inspection program to review the items listed in enclosure (1).

6. Point of Contact. The command point of contact is GySgt Crosby, Regiment Communications Chief, at 978-796-3718.

M. F. BELCHER

Dist List:
HQ Co, 25th MAR
1st BN, 25th MAR
2nd BN, 25th MAR
3rd BN, 25th MAR
4th MARDIV G6

Enclosure (1) - Information Assurance Check List for Government Network Devices

- □ Review C:\WINNT\History directory for recently visited web sites.

- □ Review temporary Internet files located at C:\WINNT\Temporary Internet Files for inappropriate material.

- □ Review quarantined files and if possible remove from device.

- □ Conduct a general file scan for inappropriate files:
  - o *.jpg
  - o *.jpeg
  - o *.mp3
  - o *.av
  - o *.tiff
  - o file suffixes for music, video, or picture files or files that are larger than 125 MB.

- □ Apply the following in the System Registry:
  - o System History setting
  - o System Online / Offline files
  - o Internet Cookies

- □ Verify virus utilities are up to date

- □ Check the system for available disk space. Report when disk space is below 100MB.